Audit Report

SUMMARY OF DOD YEAR 2000 ISSUES IV

Report No. D-2000-057 December 16, 1999

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932 or visit the Inspector General, DoD, Home Page at: www.dodig.osd.mil.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ASD(C^3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
CINC	Commander-in-Chief
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DTRA	Defense Threat Reduction Agency
DUSD(L)	Deputy Under Secretary of Defense (Logistics)
GAO	General Accounting Office
NAVAIR	Naval Air Systems Command
NAVSEA	Naval Sea Systems Command
NAVSPACECOM	Naval Space Command
NCTC	Naval Computer and Telecommunications Command
NATO	North Atlantic Treaty Organization
OMB	Office of Management and Budget
SPAWAR	Space and Naval Warfare Systems Command
TRANSCOM	Transportation Command
USFK	United States Forces Korea
USPACOM	United States Pacific Command
USSOCOM	United States Special Operations Command
Y2K	Year 2000

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

December 16, 1999

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)

SUBJECT: Summary of DoD Year 2000 Issues IV (Report No. D-2000-057)

This summary report is provided for your information. Due to the fact that this report summarizes material that has already been staffed and reported, we decided not to duplicate that staffing by reissuing a draft of this report. This report contains no recommendations; therefore, written comments are not required.

For additional information on this report, please contact Mr. James W. Hutchinson (703) 604-9060 (DSN 664-9060) (jhutchinson@dodig.osd.mil) or Ms. Mary L. Ugone (703) 604-9049 (DSN 664-9049) (mlugone@dodig.osd.mil). See Appendix B for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2000-057 December 16, 1999
(Project No. 8AS-0032.24)

Summary of DoD Year 2000 Issues IV

Executive Summary

Introduction. This is the fourth summary report issued to discuss DoD efforts to reduce year 2000 computing risks. This report summarizes audit reports, briefings, and memoranda pertaining to DoD organizations, systems, and programs and year 2000 conversion progress. The reports were issued from August 6 through December 10, 1999.

Results. Audit reports issued during the period discussed ways to strengthen the rigor of tests, clarify test results, improve reporting accuracy, and fill gaps in contingency planning. Managers and commanders generally were responsive to audit advice.

The cumulative results of the extensive audit and inspection effort to facilitate and validate DoD year 2000 conversion progress support an assessment that the Department is ready to carry out all national security missions after December 31, 1999. By early December 1999, nearly all DoD mission-critical systems were converted, all domains of the processing center platforms were ready, testing was virtually completed, and a configuration management policy was in place to control system changes that might reintroduce uncertainty. As the end of 1999 approached, there was considerable management emphasis on assuring the executability of contingency plans, which is prudent because unexpected eventualities cannot be ruled out. Also, efforts continued to ascertain the readiness of host nations, other allies, and other countries whose status could affect U.S. interests.

Management Comments. Due to the fact that this report summarizes material that has already been staffed and reported, we decided not to duplicate that staffing by reissuing a draft of this report. This report contains no recommendations; therefore, written comments are not required.

Table of Contents

DoD Year 2000 Preparedness

Audit reports issued during the period discussed ways to strengthen the rigor of tests, clarify test results, improve reporting accuracy, and fill gaps in contingency planning. Managers and commanders generally were responsive to audit advice.

The cumulative results of the extensive audit and inspection effort to facilitate and validate DoD year 2000 (Y2K) conversion progress support an assessment that the Department is ready to carry out all national security missions after December 31, 1999. By early December 1999, nearly all DoD mission-critical systems were converted, all domains of the processing center platforms were ready, testing was virtually completed, and a configuration management policy was in place to control system changes that might reintroduce uncertainty. As the end of 1999 approached, there was considerable management emphasis on assuring the executability of contingency plans, which is prudent because unexpected eventualities cannot be ruled out. Also, efforts continued to ascertain the readiness of host nations, other allies, and other countries whose status could affect U.S. interests.

Reported Results from DoD

Office of Management and Budget (OMB) Report. In the latest quarterly report to OMB, dated November 15, 1999, DoD reported that 99.5 percent of all mission-critical systems were complete. The remaining 13 systems have scheduled completion, replacement, or retirement dates ranging through December 27, 1999. The quarterly report showed that DoD was on schedule to have all mission-critical systems completed by December 31, 1999. Additionally, 98.6 percent of nonmission-critical systems were complete; and only three systems had completion dates after the December 31 conversion date. None of these three systems will be operational during the transition into the year 2000. Further, the DoD has conducted 122 end-to-end tests, consisting of 35 operational evaluations, 31 functional end-to-end tests, and 56 service integration tests.

Congressional Testimony. In his October 29, 1999, statement before the Subcommittee on Government Management, Information, and Technology, Committee on Government Reform and the Subcommittee on Technology, Committee on Science; the Deputy Assistant Secretary of Defense (Deputy Chief Information Officer and Year 2000), pointed out the tremendous scope and complexity of the Y2K problem for DoD, which has over one-third of the Federal Government's mission-critical systems. He stated that despite this challenge, the high-percentage of compliance achieved, combined with the results of end-to-end testing and operational evaluations conducted and system contingency plans tested, provide a high-degree of confidence that DoD will be able to execute the national military strategy unimpeded by Y2K related problems.

Audit Coverage

This report summarizes Y2K issues discussed in 73 audit reports issued from August through mid-December 1999. The reports primarily discussed testing, including code scanning, and contingency planning. The few remaining Y2K audits for which final reports had not been issued by December 16, 1999, either involve matters to be addressed in the last months of the conversion period, through March 2000, or will not materially affect the conclusions set forth in this summary report.

Inspector General, DoD, and General Accounting Office (GAO) auditors reviewed the planning and management of operational evaluations at seven of nine unified commands. Additionally, the auditors reviewed Y2K test planning for critical functional processes used in logistics, environmental security, procurement, health care, personnel, communications, and intelligence. Inspector General, DoD auditors reviewed the test planning for all seven critical processes used in finance and accounting. In addition, the GAO, Inspector General, DoD, and other DoD audit and inspection organizations extensively reviewed contingency planning at all organizational levels.

Management Actions on Testing

Types of Testing. The DoD Management Plan required that all mission-critical systems undergo two different levels of testing. The first level of testing validated that an individual system was Y2K compliant and performed as intended. The second level of testing ensured that a related group of systems inter-operated correctly. Higher-level testing ensured that strings of systems involved in the critical path of military operations and systems used in essential support functions were Y2K compliant. Higher-level testing was categorized as either operational evaluations, functional end-to-end tests, or service integration tests.

Audit Results. Because of the compressed time, multiple test events occurred simultaneously, which did not always allow for a sequential staging of testing. The 30 audit reports in Appendix A that addressed testing showed a variety of limitations driven by additional factors such as late availability of converted systems, poor initial mapping of inventories and interfaces, and lack of baselines. The testing managers, did, however, make good use of Defense Information Systems Agency and Military Department test and evaluation support assets.

Relative to the number of tests performed, few Y2K failures were discovered during higher-level tests, which raised concern regarding the rigor of the tests. Accordingly, DoD Components increased use of code scanning as an additional risk-mitigation effort to further minimize the risk of potential Y2K disruptions. Code scanning involved the use of automated tools to examine an applications source code to detect potential Y2K errors. Cumulatively, the testing performed at the various levels and the number of tests conducted, when supplemented by code scanning and contingency planning efforts, significantly mitigated risks of Y2K disruptions.

Management Actions on Contingency Procedures

Contingency Planning Requirements. On May 13, 1999, OMB requested that DoD and other selected Federal agencies develop an agency-level contingency plan. This contingency plan, to be developed from a headquarters perspective rather than from an individual-system perspective, was to describe the overall DoD strategy and process for ensuring readiness of key programs and functions. Additionally, the contingency plan was to follow the guidance in the GAO publication, "Year 2000 Computing Crisis: Business Continuity and Contingency Planning," August 1998. OMB also issued memoranda on October 13 and November 12, 1999, that requested updated plans be provided to OMB by October 15 and November 15, 1999, respectively.

Y2K Related Contingency Procedures. Contingency procedures have become a major focus in the DoD in the last few months of 1999 because there is still a risk that a compliant mission-critical system will be affected by a Y2K failure. Interrelations between systems and unidentified imbedded chips make it impossible to be 100 percent sure that a system will continue to function properly throughout the Y2K transition. The need for contingency procedures was recognized earlier, but was brought to the forefront with the May 13, 1999, memorandum from the OMB Director. OMB worked with the Federal agencies to refine plans as needed. This provided the agencies a chance to share lessons learned and workarounds that had been established. Additionally, testing of the contingency plans resulted in further changes in the plans. As a result of OMB requests, DoD provided a high-level business continuity and contingency plan on June 15, 1999, and provided updates to that plan on October 15 and November 15, 1999. The plan provided a broad overall strategy and process for ensuring the readiness of key programs and functions from a Department-level perspective. The plan included an explanation of how the DoD focus shifted from fixing systems in 1998 to ensuring mission capabilities through testing in 1999, and finally to ensuring continuity of operations through contingency planning.

Day One Planning. In addition to contingency and continuity of operation plans, many agencies have developed Day One plans. The plans focus on the last days of December 1999, the transition to the New Year, and the first few days of January 2000. The GAO issued guidance on Day One planning to include areas such as:

- a schedule of activities,
- personnel on call or on duty,
- contractor availability,
- communications with workforce,
- facilities and services to support their workforce,
- security, and
- communications with the public.

The Day One planning is another step that DoD Components would use to prepare for potential problems encountered during the Y2K transition. DoD included Day One planning in its high-level business continuity and contingency plan.

Contingency Plan Validation. The existence of a contingency plan for a particular system does not alleviate the risk of Y2K disruptions. It also does not guarantee that if Y2K disruptions were encountered, implementation of the contingency plan would correct the problem. Only a rigorously exercised contingency plan could be relied on in the event of a disruption. The DoD Management Plan required that contingency plans be exercised by June 30, 1999. Most DoD Components did not meet that milestone and 35 of the audit reports issued during the period raised issues concerning the sufficiency and realism of contingency planning in various DoD organizations. However, managers were generally responsive to specific findings and there has been considerable management emphasis on contingency plan validation over the last few months.

Management Actions on Consequence Management

Consequence Management Requirements. A Deputy Secretary of Defense memorandum dated February 22, 1999, provides for consequence management in the form of DoD Y2K support to civil authorities. DoD recognized two stresses on resources and operational readiness specific to the broad, near-simultaneous nature of potential problems during the Y2K transition. These stresses include:

- immediate responses that appear rational from a local perspective, but could collectively undermine the ability to execute operational missions; and

- prioritizations, which are made on the basis of requests as received, but which may quickly become outdated as higher priority requests are received for support committed elsewhere.

Because of these stresses, DoD established a set of criteria that more clearly establishes the focus and response to domestic and foreign requests for military assistance. Local commanders within the U.S. may undertake immediate unilateral, emergency response actions that involve measures to save lives, prevent human suffering, or mitigate great property damage, when time does not permit approval by higher headquarters. Except for the immediate responses, requests for DoD support will be considered only if submitted through the Federal Emergency Management Agency or appropriate offices of the Department of State. The support will be provided from forces not committed to essential national security missions, the support of standing operations plans, maintenance of domestic public health and safety, or maintenance of the economy and Nation's quality of life.

Y2K Related Events. It is the widespread belief that any Y2K disruptions in the U.S. will be temporary; however, even minor disruptions could cause major problems in local communities. For example, minor disruptions in the power supply to traffic lights could cause major transportation problems. The DoD

Consequence Management Plan assigns priorities to DoD missions and outlines the specific resources to be used to assist civil authorities in managing Y2K disruptions. Additionally, unforeseen consequences may result from implementing contingency plans. For example, a contingency plan procedure for a hospital that experiences Y2K problems may be to divert patients, but the hospital may not have the resources to support the diversion. DoD personnel not committed to essential national security missions, the support of standing operations plans, maintenance of domestic public health and safety, or maintenance of the economy and Nation's quality of life; could be called upon to assist in the implementation of the contingency plan procedure.

Management Actions on Configuration Management

Configuration Management Requirements. An August 20, 1999, Deputy Secretary of Defense memorandum outlined the limitation on configuration changes to Y2K-compliant systems. The purpose of the memorandum was to ensure that configuration changes to date-dependent, mission-critical systems do not add undue Y2K risk to, or undermine confidence in, system architectures that were determined to be Y2K compliant. To that end, the memorandum required the following procedures for obtaining approval for system configuration changes.

- Following review and approval from the Configuration Control Board, system Program Managers will submit proposed configuration changes, including Y2K risk analyses, schedules, and justification to affected Commander in Chiefs (CINC) and Principal Staff Assistants, through their program Executive Officer, Designated Acquisition Commander, or equivalent.

- CINCs and Principal Staff Assistants will have 10 working days following receipt of the change proposal to approve or disapprove implementation.

- If there are multiple affected CINCs and consensus is not reached, the Chairman of the Joint Chiefs of Staff will resolve the differences.

Additionally, any changes to tested Y2K compliant, mission-critical system architectures shall be documented in accordance with the DoD Y2K Management Plan. The memorandum covers the period from September 1, 1999, through March 15, 2000. The Inspector General, DoD is monitoring the implementation of the configuration management policy as requested by the Deputy Secretary of Defense.

Management Actions on International Outreach

Outreach Issues. Working in conjunction with other U.S. Government agencies, the DoD has made considerable progress in identifying Y2K readiness issues around the world, although considerable uncertainty is unavoidable. Audit efforts have focused primarily on DoD activities related to countries that host U.S. military installations. In four reports on host nation support issues, we discussed the efforts of various unified commands and their subordinate

commands to deal with uncertainties overseas. Although most of the details are classified, the audits confirmed that reasonable risk mitigation measures are being taken to ensure continued operation of U.S. facilities.

Summary

As of mid-December 1999, the DoD Y2K conversion effort is not yet complete, but audit results indicate that DoD's high confidence in its military capabilities is justified.

Appendix A. Summaries of Year 2000 Audit Reports, Briefings, and Memoranda

General Accounting Office

Report No. AIMD-00-30, "Defense Computers: U.S. Space Command's Management of Its Year 2000 Operational Testing," November 15, 1999. GAO testified that it found that Space Command's space control operational evaluation satisfied 16 of 21 of the key processes prescribed by the Joint Chiefs of Staff guidance to its combatant commands on managing Y2K operational evaluations. Space Command took positive actions to address the remaining five key processes. Three of the five remaining key processes were addressed during the course of the review and involved contingency plans, configuration management, and reporting issues. The remaining two key processes, which included not documenting whether test cases for most intelligence systems met performance exit criteria and not ensuring that 1 of 29 systems included in the evaluation was Y2K compliant, were addressed in response to a recommendation made at the briefing.

GAO recommended during the October 1, 1999, briefing, that Space Command amend its final report to the Joint Chiefs of Staff to recognize the uncertainties and risks associated with its failure to meet exit criteria and to confirm Y2K compliance of one system included in the operational evaluation. Space Command agreed with the recommendation and amended its final report and planned to ensure that these weaknesses were not repeated in a November operational evaluation. Space Command satisfied the intent of the recommendation.

Report No. AIMD-00-21, "Defense Computers: U.S. Transportation Command's Management of Y2K Operational Testing," November 15, 1999. GAO testified that U.S. Transportation Command's (TRANSCOM) deployment operational evaluation satisfied most of the key processes that the Joint Chiefs of Staff guidance specified. However, TRANSCOM had not satisfied certain planning, analysis, and reporting criteria associated with the evaluation's scope. The result was that the Y2K readiness of critical tasks associated with conducting a major theater war deployment was not known with sufficient certainty.

GAO recommended in its August 24, 1999, briefing that TRANSCOM amend its final reports to the Joint Chiefs of Staff to disclose scope limitations and related risks. GAO also recommended that TRANSCOM assess and selectively verify the readiness of transportation systems belonging to commercial partners.

TRANSCOM agreed with the recommendations and either implemented or initiated actions to correct the weaknesses. TRANSCOM amended its final reports on the evaluation to disclose the scope limitations. TRANSCOM was also working with its component commands to identify their major commercial

carrier business partners, to assess their readiness and risks, and to develop risk mitigation strategies. Due to these actions taken by TRANSCOM, no further recommendations were made.

Report No. AIMD-00-12, "Defense Computers: DoD Y2K Functional End-to-End Testing Progress and Test Event Management," October 18, 1999. GAO testified that each individual test event attended and reviewed for health affairs, communications, personnel, and logistics functions generally satisfied the key processes that the GAO Y2K test guides defined as necessary to effectively plan, conduct, and report on end-to-end testing. In addition, overall end-to-end efforts within three of the four functional areas were reported to be largely on schedule and completed by October 1999. However, the Communications functional area was unable to provide complete progress information on all of its 263 mission-critical systems. Communications subsequently reported that 77 mission-critical systems had completed testing, 155 systems did not require testing, and 31 mission-critical systems were considered to be behind schedule.

GAO recommended that the Secretary of Defense direct the Senior Civilian Official of the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) [ASD(C^3I)] to immediately report to the Deputy Secretary on plans for end-to-end testing of the 31 mission-critical communication systems. GAO also recommended including milestones for executing tests and reporting test results, or to otherwise justify in writing to the Deputy Secretary why any of the systems would not be included in an end-to-end test event.

DoD concurred with the findings and partially concurred with the recommendation to report to the Deputy Secretary on the status and plans for Y2K testing of the 31 mission-critical communications systems. DoD stated that during the July through August 1999 period of the review, test data was incomplete for the 31 mission-critical systems. Since then, DoD reported and provided documentation to show that Y2K testing for 14 of the 31 systems was completed, 9 systems did not process dates and were exempt from end-to-end test requirements, 4 systems were trusted systems that could not be tested in a Y2K environment due to safety, security, or operational necessity, 2 systems were developmental systems that would not be deployed before the millennium rollover, 1 system had been reclassified as a nonmission-critical system and did not require additional testing, and 1 system was scheduled to complete testing by October 15, 1999. The testing for the final system was completed on October 20, 1999.

Office of the Inspector General, DoD[1]

Report No. D-2000-053, "Year 2000 Issues of Host Nation Support for Ongoing Operations in the European Theater," December 10, 1999. The report stated that bases supporting ongoing operations in the European Theater had initiated actions to prepare operational contingency plans necessary to prepare for the Y2K transition.

The report recommended that the Commanding General, U.S. Army, Europe, and Seventh Army, ensure that the National Support Element Taszar developed and completed a Y2K contingency plan. The report recommended that the Commanding Officer, National Support Element Taszar, assign a command Y2K coordinator and complete their Y2K operational contingency plan. The report also recommended that the Commander, Operation Northern Watch, coordinate their operational contingency plan with the U.S. European Command. The report recommended the Commander, Operation Northern Watch, develop and coordinate workaround procedures. Finally, the report recommended that the Commanding Officer, Naval Air Station Sigonella, ensure that the Disaster Preparedness Plan address Y2K related risks and specific mission impacts of base operating support functional failures.

The appropriate personnel concurred with all of the recommendations. Actions were taken to address the recommendations in the report.

Report No. D-2000-052, "Year 2000 Operational Evaluations for U.S. Central Command and the Service Components," December 10, 1999. The report stated that the U.S. Central Command made significant progress in addressing its Y2K problems. The Command completed two large-scale and complex operational evaluations that demonstrated, with a very high degree of assurance, that it was ready to conduct major theater warfare in a Y2K environment. The operational evaluations tested all 11 Joint Mission Essential Tasks required to prosecute a major theater war. The Command had ongoing efforts designed to mount an aggressive effort to finalize remaining consequence management and host nation support issues.

The report recommended that the Commander in Chief, U.S. Central Command, continue to monitor the efforts of the Service Components and continue to resolve any host nation related Y2K issues.

The report also recommended that the Commander, U.S. Army Forces, Central Command; the Commander, U.S. Naval Forces, Central Command; and the Commander, U.S. Central Command Air Forces, continue their efforts to resolve the Y2K problems of the commands and to finalize any incomplete system contingency and continuity of operations plans.

Although only the Commander, U.S. Naval Forces, Central Command, provided fully responsive comments to the draft report, management's plan is to finalize Y2K conversion, thus implementing the recommendations.

[1] The full text of unclassified Inspector General, DoD, reports is available on the Internet at http://www.dodig.osd.mil and summaries of Y2K audit activity are accessible at http://www.ignet.gov.

Report No. D-2000-051, "Installation Contingency Planning and Host Nation Support in the European Theater," December 10, 1999. The report stated that six installations visited within the U.S. European Command had made considerable progress in developing contingency plans that address potential infrastructure failures related to Y2K problems and in addressing the status of their host nation service providers. The installations took actions to ensure that contingency plans were viable and fully addressed installation responsibilities. In addition, most of the scheduled testing of contingency plans was complete.

The report recommended that the Commanding General, U.S. Army, Europe, and Seventh Army:

- direct the revision of Y2K operational contingency plans to address support to the military community to include complete and clear references to existing operational contingency plans;
- complete operational contingency plans so that installations could sustain the minimum operational capabilities; and
- coordinate land transportation control systems with local government officials.

The report recommended that the Commander in Chief, U.S. Naval Forces Europe, revise operational contingency plans and continue to follow up on the Y2K status of host nation providers of electrical power, natural gas, sewage and water, and telecommunications.

The report recommended that the Commander, U.S. Air Forces in Europe, develop operational contingency plans that address support to the military community and revise operational contingency plans to include complete and clear references to operating manuals and other operational contingency plans.

The report also recommended that the Commanding General, U.S. Army, Europe; the Commander in Chief, U.S. Naval Forces Europe; and the Commander, U.S. Air Forces in Europe, complete operational contingency plan testing at all installations under their purview. The management comments were responsive.

Report No. D-2000-049, "DoD Year 2000 Contingency Plans," December 10, 1999. The report stated that audit work found mixed results in the quality of DoD contingency planning at both the system and operational levels. For 18 systems that were covered in the review, 13 systems had system contingency plans and 8 systems were mapped to operational contingency plans. The report stated that managers and commanders at all levels must continue to focus on viable contingency procedures and adequate Day One Planning to minimize the risk of Y2K disruptions. A number of DoD Components, including the Office of the Secretary of Defense Y2K Office, the Assistant Secretary of Defense (Health Affairs), the Department of the Air Force, and the Commander in Chief, U.S. Space Command reemphasized the need for adequate contingency procedures.

Although not required to comment, the Air Force Communications and Information Center stated that they concurred with the general findings of the report and that Air Force commanders would act on the concerns stated in the report.

Report No. D-2000-048, "Year 2000 Compliance Status of Biomedical Devices Included in Navy Fleet Hospitals," December 3, 1999. The report stated that the Navy Fleet Hospital Program Office incorrectly certified that none of its biomedical devices included in Navy fleet hospitals would experience Y2K related performance problems. The Fleet Hospital Program Office did not document its certification process and did not include items to be deleted from the fleet hospital inventory in its certification. The Navy Fleet Hospital Program Office also did not report its certification to higher Navy management. This resulted in fleet hospitals possibly being deployed with Y2K noncompliant biomedical devices. During the audit, the Fleet hospital Program Office initiated actions to reevaluate fleet hospital biomedical devices for compliance and to plan workarounds for Y2K noncompliant biomedical devices that would remain in the fleet hospitals after December 31, 1999.

The report recommended that the Chief, Bureau of Medicine and Surgery, assess the feasibility of the workarounds and ensure procedures are in place to effectively implement the workarounds.

The Office of the Chief, Bureau of Medicine and Surgery, concurred with the finding and recommendations stated in the report. The Office of the Chief, Bureau of Medicine and Surgery, stated the planned workarounds were adequate for the safe and effective operation of pre-positioned medical equipment and that on activation, each fleet hospital commanding officer would receive a letter with details about all Y2K noncompliant biomedical equipment.

Report No. D-2000-047, "Year 2000 Operational Evaluations for U.S. Joint Forces Command and the Service Components," December 3, 1999. The report stated that operational evaluation II verified that many of U.S. Joint Forces Command's mission-critical systems were functionally ready to operate in a Y2K environment. The further completion of phases IV and V of the operational evaluation should provide the U.S. Joint Forces Command with sufficient information to fully assess its ability to perform operations in the year 2000. The report also stated that the U.S. Army did not follow established Y2K testing criteria for its corps, divisions, and brigades. As a result, the Y2K testing did not provide the U.S. Army with the level of assurance that was intended.

The U.S. Joint Forces Command concurred with the report, stating that phases IV and V were complete and the results supported confidence in the Command's ability to perform its force provider mission in the year 2000. The U.S. Joint Forces Command also stated that it conducted oversight of Service Component testing of thin-line systems and would continue to monitor system changes. The U.S. Joint Forces Command reviewed all Service Component functional contingency plans for all identified thin-line systems and established a configuration management process to review and approve, or disapprove, all Service Components' proposed hardware and software changes to mission-critical systems. The Army did not provide comments on the draft report.

The U.S. Joint Forces Command's comments were responsive and no additional comments were required. The report requested that the Army provide comments by December 15, 1999.

Report No. D-2000-046, "Year 2000 Computing Issues Related to Health Care in DoD - Phase III," December 1, 1999. The report stated that each military facility maintains emergency preparedness plans for responding to a variety of contingencies, disasters, or emergencies. The nine military treatment facilities visited were in the process of completing, or had completed, their Y2K contingency plans.

The report recommended that the Assistant Secretary of Defense (Health Affairs) coordinate with the offices of the Military Surgeons General to supplement guidance in her October 15, 1999, memorandum. The supplement should focus on military treatment facility-wide coordination of emergency preparedness plans; departmental contingency plans; and development of day one strategies that, at a minimum, recognize resource and training requirements.

The Assistant Secretary of Defense (Health Affairs) concurred with the recommendations to supplement guidance provided in her October 15, 1999, memorandum. The Assistant Secretary of Defense (Health Affairs) issued supplemental guidance on November 17, 1999, which required each military medical department to certify its Y2K preparedness by December 20, 1999. The guidance required the certification to include a statement that all biomedical equipment, information systems, and facility components are Y2K compliant or have been removed from service. Additionally, the guidance required that the certification attest to the operational readiness of day one strategies.

Report No. D-2000-045, "Year 2000 Operational Evaluations for U.S. Special Operations Command and Its Component Commands," December 1, 1999. The report stated that the U.S. Special Operations Command (USSOCOM) made significant progress in addressing its Y2K problems. USSOCOM completed five operational evaluations to verify that most of its mission-critical systems used to support a major theater war and that its nine missions were functionally ready to operate in a Y2K environment. For mission-critical systems not included in the five operational evaluations, USSOCOM used the results of other unified command operational evaluations to verify functionality. USSOCOM and its Component commands had also integrated contingency plan testing into the operational evaluations. The report contained no adverse findings or recommendations and no management comments were required.

Report No. D-2000-043, "Air Force Level I Logistics Year 2000 End-To-End Test Planning," November 29, 1999. The report stated that the Air Force did plan to perform the verification and validation of 100 percent of mission-critical code. However, Level I end-to-end test planning for core logistics processes did not meet the requirements outlined in the DoD Management Plan and the Logistics Capstone Plan. A sufficiently detailed plan for conducting end-to-end tests for the 22 mission-critical logistics systems and 14 of the 22 core logistics processes critical to the Air Force was not developed. As of October 27, 1999, the Air Force had prepared test results for only 3 of the 7 planned test scenarios which involved 7 of the 14 core processes and 21 of the 22 mission-critical systems.

The report recommended that the Chief Information Officer, Department of the Air Force, ensure that contingency plans for the 22 mission-critical logistics systems that were included in Level I end-to-end testing be tested. The report also recommended that the Chief Information Officer ensure that a risk management plan included a risk assessment and mitigation plan for each of the Air Force core logistics processes.

The Air Force did not respond to the draft report. Therefore, the report requested that the Chief Information Officer, Department of the Air Force, provide written comments on the final report by December 15, 1999.

Report No. D-2000-040, "Navy Logistics Year 2000 End-to-End Test Planning," November 16, 1999. The report stated that the Navy end-to-end test planning for core logistics processes generally met the requirements outlined in the DoD Management Plan and the Logistics Capstone Plan. However, the Navy did not accurately track the test status of Navy mission-critical logistics systems and did not reconcile the systems with the DoD Y2K Reporting Database. For five systems, the Navy could not provide information on how or when the systems would be tested at a higher level. Further, the Navy did not provide the risk assessments prepared during the process of prioritizing logistics processes. As a result, there was no assurance that all mission-critical logistics systems would be tested as required. Also, a second code scan for the mission-critical systems needed to be performed using Crystal Systems Solutions' CodeMill, a later generation code scanner with greater capability than the one previously used. This second scan should assist in uncovering remaining Y2K errors and provide system managers the opportunity to validate and correct errors.

Additionally, adequate system contingency plans and operational contingency plans had not been written for all Navy mission-critical logistics systems, and 16 of the existing plans may not have been validated to verify that they were executable. As a result, the Navy Y2K Project Office was not effectively monitoring the completion and validation of both system contingency plans and operational contingency plans. Thus, the capability of the Navy logistics community to respond effectively to unanticipated Y2K-related disruptions of logistics systems had not yet been fully assured.

The Chief Information Officer, Department of Navy, did not comment on the draft report issued on October 6, 1999. The report requested the Chief Information Officer provide written comments to the final report by December 16, 1999.

Report No. D-2000-036, "Defense Logistics Agency Year 2000 End-To-End Test Planning," November 12, 1999. The report stated that the Defense Logistics Agency (DLA) end-to-end test planning for core logistics generally met the requirements outlined in the DoD Management Plan and the Logistics Capstone Plan. However, DLA did not conduct higher-level testing for 13 mission-critical logistics systems as required by the DoD Management Plan. Also, DLA did not document risk assessments for its core logistics processes and systems. As a result, DLA needed to ensure that its critical processes and systems would perform the operational mission in the year 2000.

The report recommended that the Chief Information Officer, DLA, develop a risk management plan for inclusion in the Deputy Under Secretary of Defense

(Logistics) [DUSD(L)] plan that includes a risk assessment and mitigation strategy for the core logistics processes, with special emphasis on those processes and systems that were not included in higher-level testing.

DLA concurred with the recommendation, stating that DLA was working with the Logistics Capstone operational test coordinator who had been tasked to complete the DUSD(L) risk assessment plan and that DLA would ensure that its core logistics processes and systems were included in the risk management strategy.

Report No. D-2000-035, "Procurement Systems Year 2000 End-to-End Test," November 9, 1999. The report stated that DLA conducted end-to-end tests of its mission-critical procurement systems, but did not test any of the system's external interfaces. Without additional checks, the Director, DLA, could not ensure that the procurement process would not be adversely affected by data from external interface partners.

The report recommended that the Director, DLA, check all external interfaces of the Mechanization of Contract Administration Services procurement system to ensure that the window being used to interpret the century from the year is clearly defined and successfully communicated to the interface partners.

DLA concurred with the recommendation and agreed to conduct a risk mitigation study of all external interfaces between the Mechanization of Contract Administration Services procurement system and the systems that use it. The external interface testing was ongoing.

Report No. D-2000-033, "Army Logistics Year 2000 End-to-End Test Planning," November 5, 1999. The report stated that the Army end-to-end test planning for mission-critical logistics processes generally met the requirements outlined in the DoD Management Plan and the Logistics Capstone Plan. Five critical core processes (requisition, shipment, receipt, inventory control, and asset status) were identified and planned for testing by the Army. However, the Army did not document the risk assessments performed during the process of prioritizing logistics processes for inclusion in end-to-end testing as required by the DoD Management Plan and the Logistics Capstone Plan. A lack of sufficient information contributed to delays in completing the DUSD(L) risk management plan for all core logistics processes.

The report recommended that the Chief Information Officer, Army, develop a risk management plan that includes a risk assessment and mitigation plan for each of the core logistics processes. The risk management plan should be based on probability of occurrence and consequences of occurrence and list the mitigation for a particular risk.

The Army concurred with the recommendation, and stated that it was participating with the other Services to develop a core logistics process risk assessment and mitigation plan. The DUSD(L) serves as the lead for the effort and Component data would be reflected in the final integrated product.

Report No. D-2000-032, "Year 2000 Status of the Compliance Monitoring and Tracking System," November 5, 1999. The report stated that the draft report questioned the ability of the Compliance Monitoring and Tracking System to operate successfully in the year 2000 because documentation provided by the Defense Threat Reduction Agency (DTRA) did not support the system certification. Additional work performed and additional documentation provided in response to the draft report provided new and adequate assurance that the Compliance Monitoring and Tracking System would operate successfully in the year 2000.

DTRA comments to the report were considered to be responsive. DTRA also provided additional information necessary for Y2K certification. Specifically, DTRA provided a letter from the Program Manager that stated no additional Compliance Monitoring and Tracking System interfaces beyond those identified by the auditors existed, and that interface agreements had been prepared for all interfaces identified. Clarification of interface test documentation was provided, as were functional end-to-end testing documentation and justification for the certification level reported.

Report No. D-2000-029, "Year 2000 Contingency Planning and Operational Evaluation Reporting By U.S. Forces Korea," November 1, 1999. The report stated that U.S. Forces Korea (USFK) and its subordinate organizations made significant progress toward ensuring mission capability through the Y2K transition period. However, USFK and its subordinate organizations had not finalized and tested all Y2K contingency plans supporting critical missions. Also, workarounds for Y2K contingency plans had not been prioritized or fully coordinated.

USFK concurred with the finding and recommendations addressing contingency planning efforts. USFK stated corrective actions were ongoing to finalize and exercise all Y2K contingency plans supporting critical missions and systems. USFK also stated the contingency plans were being reviewed to ensure their adequacy, that the plans were supported by viable and sufficient resources, and that plans were in place to prioritize and coordinate resource requirements to enable the simultaneous accomplishment of critical missions. USFK partially concurred with the finding and recommendations addressing its operational evaluation reporting, and stated that corrective actions were taken to improve its training and procedures and adjustments in the preparation of the second operational evaluation had been made. Comments from USFK were responsive; therefore no further comments were required.

Report No. 00-026, "Joint Operation Planning Year 2000 Issues," October 27, 1999. The report stated that the level of certification for the Joint Operation Planning and Execution System was incorrect and the system was at an increased risk of not being able to continue operations in the event of a Y2K disruption. The Joint Operation Planning and Execution System tests revealed ambiguous display and printing of dates and Joint Operation Planning and Execution System segments contained software that was not Y2K compliant. Also, the Joint Staff did not have a complete Y2K operational contingency plan to continue crisis action planning and operations support in the event of a Joint Operation Planning and Execution System failure because of Y2K problems.

The Joint Staff and TRANSCOM comments to the draft report were responsive. Defense Information Systems Agency (DISA) comments were partially

responsive. DISA had not identified a Global Command and Control System baseline that would be in use at all user locations, that had all segments successfully tested by DISA, was tested at least twice in end-to-end tests or unified command operational evaluations, and was independently tested with all external system interfaces, before transitioning to the year 2000. The report requested that DISA reconsider its position and provide comments on the final report by November 24, 1999. DISA comments were received November 23, 1999, and were considered to be responsive. No unresolved issues remain.

Report No. 00-025, "End-to-End Testing for Personnel Systems," October 26, 1999. The report stated that the Army, Navy, Air Force, and Marine Corps were conducting end-to-end testing of their personnel systems but that more was needed to be done to provide assurance of Y2K compliance. The Navy did not begin its testing until September 1999, which increased its risk that it would not complete the end-to-end testing and analysis of that testing before the year 2000. The Navy remained confident the testing plan would be carried out in time. The Air Force end-to-end test involving the Defense Civilian Personnel Data System was not as rigorous as required by the DoD Y2K Management Plan. The end-to-end test as conducted did not provide additional assurance that Y2K risk for the Defense Civilian Personnel Data System had been reduced. The Air Force chose to use test data that it saved from the system certification test of the Defense Civilian Personnel Data System instead of evaluating it in either a functional area Y2K end-to-end test or a Service-sponsored Y2K system integration test.

The report recommended that the Deputy Chief of Naval Personnel require that interface reexamination procedures be performed for all Navy mission-critical personnel systems and that advanced automated scanning tools be used to examine all of the application software for those systems.

The Chief of Naval Personnel, Bureau of Naval Personnel, concurred and stated that end-to-end testing started September 4, 1999, and would be completed by the end of October. The Navy also stated that code scanning was in process, interface testing was a continuous ongoing process, and that draft contingency of operations plans were developed. The Navy was confident that the personnel systems would operate after January 1, 2000. The Air Force disagreed that its testing was not as rigorous as required by the DoD Y2K Management Plan. The Navy comments were considered to be responsive and corrective actions were complete.

Report No. 00-021, "Air Force Logistics Year 2000 End-to-End Test Planning," October 26, 1999. The report stated that the Air Force end-to-end test planning for mission-critical logistics processes generally met the requirements outlined in the DoD Management Plan and the Logistics Capstone Plan. However, the Air Force did not accurately track and report three mission-critical systems subject to higher-level tests. Also, the Air Force missed an opportunity to test contingency plans for mission-critical systems during Level II end-to-end testing. Further, the Air Force did not document the risk assessment and mitigation plans for core logistics processes. There was an increased risk that all mission-critical logistics systems and contingency plans would not be tested as required.

The Air Force concurred with the recommendations to test contingency plans for systems that were included in Level II end-to-end testing and to determine the status of three mission-critical systems that lacked higher-level testing. The Air Force nonconcurred with the recommendation to develop a risk management plan for core logistics processes. The Air Force stated that responsibility for developing the risk management plan was assigned to the Operational Test Coordinator within the office of the DUSD(L).

Air Force comments were not fully responsive. The Chief Information Officer, Department of the Air Force, should have ensured that the development of a risk management plan for Air Force core logistics processes was included in the DUSD(L) overall risk management plan.

Report No. 00-018, "Defense Travel Pay Year 2000 End-to-End Testing," October 22, 1999. The report stated that the travel pay end-to-end test event leader did not use the Defense Finance and Accounting Service (DFAS) Y2K Master Plan developed by the Y2K office, but instead attempted to prove that previous system-level tests made on the travel pay system would qualify as end-to-end testing. Previous tests had been made only on systems in the travel pay business process and were made using non-Y2K compliant systems. Also, test scenarios were not developed for all systems in the travel pay business process.

The Director for Information and Technology, DFAS, concurred with the report and stated that four scenarios were developed to test the travel pay business process and that the scenarios identified all the systems involved. Further, additional Y2K testing was completed after the Standard Finance System Redesign (Subsystem 1) disbursement system was certified as Y2K compliant. DFAS, with assistance of the Joint Interoperability Testing Command, refined its approach to end-to-end testing; developed standard documentation procedures that provide reasonable assurance that risks from Y2K problems would be mitigated; and initiated additional live testing.

Report No. 00-017, "Defense Military Pay Year 2000 End-to-End Testing," October 21, 1999. The report stated that DFAS plans for conducting military pay end-to-end testing were not in accordance with the DFAS Y2K End-to-End Master Plan. Specifically, the end-to-end test plans did not:

- provide for testing all critical dates,
- provide for testing in a simulated environment with an analysis of the risks involved,
- require baselines as stated in the Master Plan,
- include a standard methodology for tracking the tests, and
- provide for a risk assessment and management program.

The report recommended that DFAS take alternative measures to mitigate the risk that military pay systems will be unable to successfully process data in a Y2K environment. Alternative measures may include using code scanners, expanding the contingency plans, and performing supplementary end-to-end tests.

The Director for Information Technology, DFAS, concurred with the recommendations and stated that DFAS had the Joint Interoperability Test Command independently review the end-to-end testing. The Director also stated that additional contingency plans were drafted and an independent contractor had performed code scanning of the Defense Joint Military Pay System and that other military pay systems would be scanned before November 30, 1999. The Joint Interoperability Test Command completed its review September 21 through October 1, 1999, and no unresolved issues remain.

Report No. 00-015, "Audit of Year 2000 Higher Level Testing Schedule Data Reported to DoD," October 20, 1999. The report stated that the Services and DoD agencies had made progress scheduling and conducting higher-level testing on all mission-critical date-dependent systems. However, additional efforts were needed to complete the DoD Y2K testing database. The database needed scheduling input for 46 Navy systems and one DTRA system.

The Principal Director for the DoD Y2K Program Office, ASD(C^3I) concurred with the conclusion in the draft audit report. The Principal Director stated that his office was working with the Services and agencies to populate the DoD test database and to ensure that the information provided was current and correct.

Report No. 00-014, "Intelligence Functional Area Year 2000 Higher Level Test Planning," October 20, 1999. The report stated that as of July 27, 1999, the DoD community had 395 mission-critical systems of which 141 had completed higher-level tests, 111 were scheduled for testing, and 143 did not require testing because the systems were standalones or were not date dependent. Of the 252 systems requiring higher-level testing, 34 required two tests and 218 required one test. The U.S. Intelligence Y2K Working Group, as the primary Y2K coordination and issue resolution body for U.S. Intelligence, effectively tracked, monitored, and reported higher-level testing of mission-critical systems within the DoD intelligence community. To validate information reported by the U.S. Intelligence Y2K Working Group, DoD reviewed higher-level test planning efforts of each DoD Intelligence Component. All DoD Intelligence Components appropriately planned higher-level tests for their mission-critical systems, although not all were able to complete testing before the target date of September 30, 1999. The report contained no recommendations; therefore, no comments were required.

Report No. 00-007, "Defense Transportation Pay Year 2000 End-to-End Testing," October 12, 1999. The report stated that DFAS made significant improvements in end-to-end testing of the transportation pay systems. The transportation pay systems should continue to operate as intended in the year 2000. In addition, tests were successfully performed with the Federal Reserve Bank on September 15, 1999.

Management actions were responsive to suggestions made during the review of end-to-end tests. The report contained no recommendations.

Report No. 00-006, "Defense Disbursing Year 2000 End-to-End," October 12, 1999. The report stated that the DFAS Y2K Project Office developed a sound overall methodology for conducting end-to-end testing. However, unless interfaces were tested between disbursing systems and other systems, inconsistencies or incomplete test results may occur if disbursing was

tested as a separate event because the disbursing process is an integral part of each of the other six core processes. In addition, DFAS Headquarters Disbursing Business Area Y2K End-to-End Test Plan (the Disbursing Event Plan) was deficient in describing the test procedures, processes, and resources required for conducting end-to-end tests. Also, the Disbursing Event Plan lacked a master schedule of testing dates and criteria for successful completion of end-to-end testing. The Disbursing Event Plan also lacked critical requirements for testing the disbursing event, procedures for developing test data and a baseline, consistency in the use of test scenarios, and standardization in the selection of a test methodology. Consequently, the Disbursing Event Plan and the disbursing systems test plans for end-to-end testing may not have fully ensured that the processing and disbursing of payments would continue unaffected in the year 2000.

The report recommended that the Director, DFAS, initiate steps to include the Standard Negotiable Items Processing System in the end-to-end testing process and initiate alternative measures to mitigate the risks of disbursing systems not being able to process data due to Y2K related failures. Alternative measures may include expanding event contingency plans, using code scanners, or performing supplementary end-to-end tests of the event. DFAS concurred with the report and stated it would code scan the disbursing systems.

Report No. 00-004, "U.S. European Command Year 2000 Operational Readiness," October 8, 1999. The report stated that the U.S. European Command had completed its operational evaluations of intelligence, land, sea, and air operations. In addition, the U.S. European Command, in coordination with the Joint Staff, the Services, and the Principal Staff Assistants, reviewed the results of the Service-sponsored systems integration tests and the functional area end-to-end tests and verified that the systems tested were functionally ready to operate in a Y2K environment. However, the U.S. European Command needed to continue to take action through its risk mitigation efforts to reduce any potential impact on its ability to conduct peacekeeping operations caused by Y2K interoperability problems with North Atlantic Treaty Organization (NATO) and coalition forces.

The report recommended that the U.S. European Command's risk mitigation efforts include a focus on the Y2K compliance of NATO and coalition forces' mission-critical systems supporting peacekeeping operations in the European theater.

The U.S. European Command agreed with the findings in the report and stated that its risk mitigation efforts contain contingency planning for infrastructure and host nation support risks and life support of military communities. Also, assurance of continuity of operations of ongoing operations and engagement with NATO and coalition forces' risk mitigation activities was included in the risk mitigation efforts. However, in light of the limited information available on the actual status of other nations' command and control systems, planning by the U.S. European Command and its Service Components would continue to include the risk that all or parts of those systems may not be available or may not be Y2K compliant.

The U.S. European Command Y2K task force and Supreme Headquarters Allied Powers Europe Y2K Program Management Office were exchanging information on the status of systems as data became available.

Report No. 00-002, "Year 2000 End-To-End Testing: Logistics Capstone Plan," October 1, 1999. The report stated that the end-to-end test planning for the inter-Component mission-critical logistics processes generally met the requirements outlined in the DoD Management Plan. The DUSD(L) in conjunction with the Logistics Y2K Interface Assessment Working Group prioritized the logistics processes and data flows that were included in testing based on criticality to the warfighter. However, the DUSD(L) did not formally document the risk assessment process that was required to be conducted as part of identifying and prioritizing the core logistics processes. Also, the DUSD(L) did not systematically monitor the content of the CINC operational evaluations or Service integration tests to ensure that any systems or processes not covered were identified and included in the logistics functional end-to-end tests.

The report recommended the DUSD(L) develop a risk management plan that includes a risk assessment and mitigation plan for all logistics processes and their mission-critical systems, with emphasis placed on risks associated with the selection of the five mission-critical processes. The report also recommended the Chief Information Officers of the Army, the Navy, and DLA implement the DUSD(L) requirement to perform an independent verification and validation of 100 percent of the software code that impacts the mission-critical logistics processes.

The DUSD(L) concurred with the recommendations. The DUSD(L) stated that a risk assessment had not been completed and mitigation actions that resulted from the assessment would be worked within the Logistics Y2K Interface Assessment Working Group. DLA partially concurred with the recommendation and stated that it had undertaken a code scanning program for its mission-critical logistics systems and had put budgetary and administrative provisions in place to scan its mission-critical systems.

The DUSD(L) and DLA comments were responsive. As of the date of this summary report, Army and Navy action was still incomplete.

Report No. 00-001, "Year 2000 Issues Within the U.S. Pacific Command's Area of Responsibility, Alaskan Command," October 1, 1999. The report stated that the Alaskan Command had taken actions to ensure mission capability through the Y2K transition period and had began Y2K outreach coordination with civil authorities and other Federal agencies in Alaska. The remaining five mission-critical systems were scheduled to be Y2K compliant by October 30, 1999. Contingency plans were prepared and executed for all mission-critical systems. However, the Alaskan Command needed to prioritize workarounds to ensure critical mission accomplishment if resources proved inadequate. The Alaskan Command also needed to improve the coordination of workarounds outlined in its various Y2K contingency plans to ensure sufficient resources were in place if simultaneous workaround measures had to be implemented.

In contrast, U.S. Army Alaska started its Y2K conversion late and as a result needed to complete five contingency plans, exercise those plans, prioritize workarounds to ensure critical mission accomplishment if resources proved inadequate, and coordinate workarounds to ensure sufficient resources were in place if simultaneous workaround measures had to be implemented.

The report recommended that the Commander, Alaskan Command, continue to track and monitor the renovation of the noncompliant systems and finalize the prioritization and coordination of workarounds outlined in its contingency plan in case of Y2K difficulties. The report also recommended that the Commander, U.S. Army Alaska, implement vigorous Y2K efforts, including assessment verification, contingency planning, and workaround prioritization and coordination efforts, to ensure accomplishment of the mission-critical functions.

The Commander, Alaskan Command, concurred with the recommendations and stated corrective actions had been taken. U.S. Army Alaska concurred and nonconcurred with elements of the recommendations and stated that the report did not accurately indicate U.S. Army Alaska Y2K responsibilities and readiness. The Commander, Alaskan Command, comments were responsive, and U.S. Army Alaska comments in response to the final were responsive. No unresolved issues remain.

Report No. 99-262, "Audit of the Year 2000 Mission-Critical Non Date-Dependent Systems," September 30, 1999. The report stated that 130 of the Air Force's systems were reviewed and 126 were properly classified as nondate-dependent. The four systems remaining were date-dependent and were reclassified as mission-essential. In addition, they were tested to ensure Y2K compliance. The Department of Defense had a 90 percent confidence that the mission-critical non date-dependent systems in the DoD Y2K database were accurately classified as non date-dependent and did not require higher-level testing. The report contained no adverse findings and no management comments were required.

Report No. 99-261, "Preparation of the Joint Surveillance Target Attack Radar System Common Ground Station for the Year 2000," September 29, 1999. The report stated that the Joint Surveillance Target Attack Radar System Common Ground Station Program Office actively planned and managed Y2K issues to provide reasonable assurance that the Joint Surveillance Target Attack Radar System Common Ground Station would be able to properly process date-dependent information before, on, and after January 1, 2000. However, the Joint Surveillance Target Attack Radar System Common Ground Station Y2K Management and Contingency Plan did not include predetermined actions to streamline decision making if an unexpected Y2K disruption occurred.

The report recommended that the Program Manager, Joint Surveillance Target Attack Radar System Common Ground System, update the Y2K contingency plan to identify predetermined actions that would enable resumption of mission operation at the earliest possible time and in the most cost effective manner if the Common Ground Station incurs mission interruptions due to Y2K incidents. The Executive Officer, Electronic Warfare and Sensors, concurred with the recommendation and indicated that actions had been implemented to update the Y2K contingency plan.

Report No. 99-259, "Defense Civilian Pay Year 2000 End-to-End Testing Event Plans," September 28, 1999. The report stated that Civilian pay event planners took the initiative to develop end-to-end event plans well before requirements were defined for DFAS as a whole, and to develop a sound methodology for end-to-end testing of civilian pay. However, DFAS Headquarters did not require revisions to the civilian pay event plans as overarching guidance was issued. The civilian pay event plan lacked

requirements for data collection and data analysis. Although only one thread of the civilian pay end-to-end testing event had been completed (with confirmations received from all of the output partners in the thread), the civilian pay event planners had tested the Defense Civilian Pay System segment for six of the seven threads.

The report recommended that the Director, DFAS, require the civilian pay event leader, prior to the completion of end-to-end testing and any re-testing, to document uniform detailed data collection and data analysis procedures that allowed for uniform, standardized testing between participating systems.

The Director, Information and Technology, DFAS, concurred with the recommendation, and stated that the civilian pay data collection and analysis methodologies would be documented and provided to DFAS by October 29, 1999. The Director stated that because the requirements for data collection and data analysis plans were published after the civilian pay end-to-end test had began, the event did not contain the plans.

The report considered DFAS comments to be generally responsive. The Joint Interoperability Testing Command, DISA, was to review the civilian pay event test results in October 1999.

Report No. 99-255, "Year 2000-Sensitive Property Reutilized, Transferred, Donated or Sold," September 15, 1999. The report stated that DoD was transferring property that may not have been Y2K compliant to other Federal and State agencies; donating it to educational institutions, governmental humanitarian programs, or nonprofit organizations; and selling it to the general public. Recipients of the transferred, donated, or sold property may have been exposed to various levels of risk.

The Office of the ASD(C^3I) concurred with the recommendation to clarify disposal guidance and developed appropriate guidance for inclusion in the DoD Y2K Management Plan. Also, the property mutilated by the disposing organization would no longer be identified as Category 1 defective property but would be identified as scrap.

The DLA did not concur with the recommendation to suspend disposal actions of all excess and surplus property, stating that the Agency had been tasked to assess Y2K sensitivity of all items of supply and was in the final phases of completing its assessment. However, DLA agreed to suspend all disposal actions regarding biomedical equipment until such equipment was determined to be Y2K compliant.

The report requested that DLA reconsider its nonconcurrence on the recommendation to suspend disposal actions for other than biomedical equipment until Y2K compliance was established. DLA refused to do so and followup action is ongoing.

Report No. 99-254, "Year 2000 Issues Within the U.S. Pacific Command's Area of Responsibility, Operational Evaluation Planning by U.S. Forces Korea," September 16, 1999. The report stated that the USFK approach to evaluate the Combined Forces Command ability to execute major theater warfighting operations in a Y2K environment was fundamentally sound and

should result in reasonable assurance that the integrated systems identified in the thin-lines for critical tasks would operate correctly. However, an evaluation of nonintegrated Republic of Korea systems essential to tasks critical to the Combined Forces Command warfighting capability was not performed. Failing to integrate an evaluation of Republic of Korea systems could have resulted in USFK failing to have critical information needed to minimize risk to the Combined Forces Command warfighting mission capability.

The Commander in Chief, USFK, who also serves as Commander in Chief, Combined Forces Command, concurred with the report recommendations and stated that the recommendations had been implemented. USFK stated that it had identified and addressed essential nonintegrated Republic of Korea systems and capabilities. Additionally, USFK stated it had established communications channels with the Republic of Korea, Ministry of National Defense, to address and continually review Republic of Korea Y2K efforts, and integrate the assessments of Republic of Korea Y2K efforts in the USFK operational evaluation results.

Report No. 99-253, "Environmental Security Year 2000 End-To-End Tests," September 15, 1999. The report stated that DLA had not planned and performed effective end-to-end tests for environmental security automated information systems reported as being mission-critical. The tests lacked an adequate number of systems to test the function of environmental reporting. Also, DLA had not completed system-level contingency plans to address procedures for minimizing disruptions in the event of Y2K related system failures.

The report recommended that the Director, DLA, complete system-level contingency plans for the environmental security automated information systems.

Because DLA did not provide comments to the draft report, comments in response to the final report were requested by October 15, 1999. Contingency plans were furnished with the management comments to the final report. No unresolved issues remain.

Report No. 99-252, "Year 2000 Status of the Centralized Accounting and Financial Resource Management System, Defense Threat Reduction Agency," September 15, 1999. The report stated that the Centralized Accounting and Financial Resource Management System was not planned for inclusion in any type of higher-level testing as required by the DoD Y2K Management Plan for all date dependent mission-critical systems not operating in a stand-alone environment. The Centralized Accounting and Financial Resource Management System was not a stand-alone system and therefore, required a higher-level test.

DTRA was developing a new action plan for the implementation, testing, and recertification of the Centralized Accounting and Financial Resource Management System to include higher-level testing as required by the DoD Y2K Management Plan. The implementation of this new action plan would have a positive effect in reducing the risk that the Centralized Accounting and Financial Resource Management System would fail or have an adverse impact on other DoD systems because of Y2K related difficulties.

The report recommended that the Comptroller, DTRA, verify that the Centralized Accounting and Financial Resource Management System Action Plan was completed on time and fulfilled the testing requirements of the DoD Management Plan.

DTRA concurred with the recommendation. DTRA stated that it believed that the Centralized Accounting and Financial Resource Management System Action Plan met the DoD requirements in the Y2K Management Plan and would continue to carry out the necessary actions stated in the Plan. All requirements in the Centralized Accounting and Financial Resource Management System Action Plan were completed; no unresolved issues remain.

Report No. 99-246, "Defense Contractor and Vendor Pay Year 2000 End-to-End Testing," September 3, 1999. The report stated that DFAS event and test plans for end-to-end testing of contractor and vendor pay functional processes needed improvement. The event and test plans lacked verified assumptions, documented and explained testing constraints, and requirements for data collection and data analysis. The plans also initially lacked clearly defined test environments, test scenarios, exit criteria, baselines, and roles and responsibilities.

The report recommended that the Director, DFAS:

- verify the assumptions and fully explain and document constraints that impact end-to-end testing,
- prepare and document a detailed data collection and analysis plan prior to testing,
- document clearly defined test environments and associated risks,
- establish and document test scenarios and exit criteria,
- document a baseline for the Computerized Accounts Payable System thread prior to testing, and
- ensure that the Y2K End-to-End Project Office oversees compliance with the DFAS Master Plan.

DFAS did not alter the Master Plan Checklist as previously recommended by the Inspector General, DoD. DFAS cited the fact that because each business application has a normal testing practice established, the use of checklists was not mandatory, and DFAS preferred to keep the use of checklists optional.

Management concurred with all other recommendations and stated that improvements were made. The DFAS Y2K End-to-End Project Manager periodically conducted in-process-reviews to assess progress and compliance. DFAS initiated and completed the necessary steps to correct the Y2K issues stated in the report.

Report No. 99-245, "Year 2000 Issues Within the U.S. Pacific Command's Area of Responsibility, Operational Evaluation Planning at U.S. Pacific Command Headquarters," September 2, 1999. The report stated that the approach U.S. Pacific Command (USPACOM) developed to evaluate its ability to execute joint task force and major theater war deployment operations within its area of responsibility in a Y2K environment was fundamentally sound. When USPACOM operational evaluations were combined with assessments made during Service integration tests, USPACOM would have the information needed to fully assess whether it could execute joint task force and major theater war deployment operations in a Y2K environment. The report contained no recommendations.

Report No. 99-241, "Reported Year 2000 System Certification Levels," August 23, 1999. The report stated that the detailed DoD Y2K system certification-level data reported into the DoD Y2K Database was unreliable because of inconsistencies in certification level definitions. The DoD Y2K Management Plan encouraged but did not require the use of its sample Y2K compliance checklist. In addition, the DoD Y2K Management Plan included inconsistent definition of certification levels which created the problem that even if the Components converted their unique certification levels to equivalent DoD certification levels before reporting into the DoD Y2K Database, there was no way to determine which DoD policy was used as the guideline.

The report recommended that the Office of the ASD(C^3I):

- correct the certification-level reporting inconsistencies contained in the DoD Y2K Management Plan, and

- notify the DoD Component data owners to verify and correct, as needed, the information contained in the DoD Y2K Database using the updated reporting guidance.

The office of the ASD(C^3I) concurred with the recommendations, and stated that the Y2K Program Office corrected the certification-level inconsistencies. The Y2K Program Office also coordinated with the DoD Components to ensure certification-level information was correctly reported.

Report No. 99-240, "Year 2000 Issues Within U.S. Special Operations Command and Its Component Commands," August 23, 1999. The report stated that USSOCOM headquarters was making progress in addressing its Y2K problems. However, the level of Y2K efforts within USSOCOM and its Component commands varied in scope and was still evolving. USSOCOM had not developed an adequate control process for its Y2K program. USSOCOM and its Component commands had not provided adequate guidance for planning and testing criteria of its owned mission-critical and thin-line systems.

USSOCOM concurred with all report recommendations with the exception of reconciling the reporting of Y2K status of mission-critical systems between the Command Control and Information contractor and USSOCOM, and expediting planning of operational evaluation and providing information to the Component commands. The Joint Staff neither concurred nor nonconcurred, and stated that USSOCOM would evaluate the special operations missions during its five scheduled operational evaluations. USSOCOM comments were fully responsive and no additional comments were requested.

Report No. 99-238, "Defense Information Systems Agency Megacenter Support of the Year 2000 Functional End-to-End Testing Requirements," August 20, 1999. The report stated that the DISA Megacenter had exercised due diligence in supporting Y2K functional end-to-end testing requirements for the finance, logistics, and personnel functional areas. To support functional testing requirements, 38 test domains were established by DISA and would be available through December 31, 1999. Additionally, for scheduling and planning resource requirements, DISA had asked functional end users to finalize and submit functional testing requirements.

Report No. 99-235, "Year 2000 Status of the Defense Threat Reduction Agency Nuclear Weapon Information Tracking Systems," August 19, 1999. The report stated that DTRA exercised due diligence in validating the Y2K readiness of its mission-critical Nuclear Weapon Information Tracking Systems.

For the Nuclear Management Information System, the Nuclear Weapons Contingency Operations Module, and the Special Weapons Information Management System, DTRA:

- assessed the Y2K compliance of the system inventory,
- conducted Y2K system verification and certification testing,
- assessed the system interfaces,
- developed and tested its system contingency plans,
- participated in the first of the two required operational readiness tests, and
- scheduled a second operational readiness test.

The report contained no recommendations and concluded that DTRA had obtained a reasonable level of assurance that the functions performed by the systems will function after the year 2000.

Report No. 99-234, "Year 2000 Status of the Nuclear Inventory Management and Cataloging System," August 19, 1999. The report stated that DTRA has adequately assessed Y2K issues to ensure Y2K compliance of the Nuclear Inventory Management and Cataloging System, but had not fully documented all relevant information. The Nuclear Inventory Management and Cataloging System inventory had not shown the version of the product used; the test plan and report had not adequately described test procedures, expected results, and actual results; and the contingency plan was not practical.

DTRA supported the intent of recommendations regarding the need to improve documentation for the inventory list, testing documentation, Y2K compliance checklist, and a Y2K contingency plan. DTRA provided an After Action Plan of the lessons learned, a Test Analysis Report, and an updated Nuclear Inventory Management and Cataloging System and Operational Contingency Plan. However, DTRA did not agree that the certification level was inaccurate.

DTRA believed it accurately reported the certification level in accordance with the DoD Y2K Management Plan. The DoD Y2K Program Office agreed to review the certification coding issue.

Report No. 99-232, "Year 2000 Issues Within U.S. Atlantic Command and the Service Components," August 16, 1999. The report stated that the U.S. Atlantic Command headquarters had made progress in addressing its Y2K problems. However, coordination among the Component commands needed improvement to ensure all Y2K issues were properly addressed. Also, U.S. Atlantic Command and its Component commands needed to intensify efforts in dealing with Y2K issues because of the limited time that remain.

The Commander in Chief, U.S. Atlantic Command; the Commander, U.S. Army Forces Command; the Commander in Chief, U.S. Atlantic Fleet; and the Commander, Air Combat Command; concurred with the report recommendations. Each provided specific details on procedures used to act on the recommendations.

Report No. 99-231, "Year 2000 Application Testing at the Defense Finance and Accounting Service," August 10, 1999. The report stated that the eight DFAS mission-critical systems met DFAS requirements for application testing during the validation phase of the Y2K conversion process. System managers planned, executed, and coordinated system testing to ensure that the systems processed and exchanged date and date-related information accurately in a Y2K environment. However, for 30 of 40 DFAS mission-critical systems, DFAS had insufficient information on the Y2K status of computer processing domains owned and operated by DISA.

The report recommended that the Director, DFAS, require system managers to ascertain from the Inventory/Asset and Configuration Management System, the Y2K compliance status of each hardware and software product in individual test domains prior to determining level 3 compliance for any DFAS systems that resided on the domain owned and maintained by DISA.

The Director, Information and Technology, DFAS, partially concurred, and stated that DFAS and DISA would, at a corporate level, jointly review the compliance status of each test domain at the time of Level 3 certification testing for DFAS systems. The Director also stated that although the Inventory/Asset and Configuration Management System may be used to verify the compliance of some products, DFAS would not require individual system managers to use that system.

Report No. 99-229, "Preparation Of The Global Positioning System For Year 2000," August 9, 1999. The report stated that the Global Positioning System Program Office and the 2nd Space Operations Squadron actively planned and managed Y2K and End-of-Week rollover issues for the Global Positioning System Operational Control Segment. The Space Segment's satellite vehicles did not use conventional time and date data and were Y2K compliant. However, contingency and operational plans were incomplete for the Operation Control Segment.

The report recommended that the Commander, Air Force 50th Space Wing update the Operational Control Segment's operational contingency plan to

include start dates for precontingency actions, End-of-Week rollover procedures, and point of contact lists for internal and external support staff.

The report also recommended that the Program Manager, Global Positioning System:

- develop, document, and test Y2K workaround procedures and implement them if the Integrated Mission Operations Support Center is not completed, tested, and installed before December 31, 1999, and
- develop and test contingency plans for the Operational Control Segment to include updated point-of-contact lists, start dates for precontingency actions, and additional training and resource needs.

The Assistant Secretary of the Air Force, in coordination with the Commander, Air Force 50th Space Wing, and the Program Manager, Global Positioning System, concurred with all of the report recommendations. The Global Positioning System Program Office and the 50th Space Wing took the necessary actions to address the recommendations in a quick and decisive manner.

Report No. 99-228, "Year 2000 Status of the Commodity Command Standard System," August 6, 1999. The report stated that in conjunction with representatives from the operational sites, the Logistics Systems Support Center, adequately tested and certified the Commodity Command Standard System as Y2K compliant and developed a reasonable system contingency plan. However, several issues may cause an increased risk of Y2K related failure, including interface memoranda of agreement, system and operational contingency plans, and pre-Y2K system releases. Therefore, actions were needed by the Commodity Command Standard System to reduce the risk of Y2K related failures.

In coordination with the Logistics Systems Support Center, the Army Material Command concurred with all the report recommendations. The contingency plans for the Commodity Command Standard System were tested on June 29, 1999. The Army Material Command Deputy Chief of Staff for Logistics, published Guidelines for the development and testing of the operational contingency plans for the Commodity Command Standard System on May 27, 1999. The Logistics Systems Support Center initiated action to revalidate each memorandum of agreement in accordance with the new DoD guidance published after initial agreements were completed.

Army Audit Agency

Memorandum Report No. AA 00-84, "Audit of Year 2000 Facility Infrastructure (Non-Information Technology) at Fort Stewart," November 30, 1999. The memorandum report stated that responsible personnel were addressing Y2K risks to ensure continuity of operations for mission-essential functions. In addition, installation personnel took actions to correct discrepancies noted during testing of facility infrastructure.

The Army Audit Agency suggested that the Garrison Commander:

- prepare a plan of action to consolidate installation operational contingency plans and incorporate Y2K issues,
- prioritize installation potable water distribution in the event of water contamination or shortage, and
- monitor the installation hospital status of replacing noncompliant biomedical equipment and ensure that adequate backup procedures are incorporated within the installation overall continuity of operations plan.

The Garrison Commander concurred with the suggestions and stated that actions had been taken to address those suggestions.

Memorandum Report No. AA 00-83, "Audit of Year 2000 Facility Infrastructure (Non-Information Technology) at Fort Campbell," November 30, 1999. The memorandum stated that responsible personnel were addressing facility infrastructure for Y2K impact. Although planning was not completed during the audit, actions were ongoing to complete Army guidance for contingency planning. In addition, actions had been taken to correct discrepancies noted during testing of facility infrastructure.

The memorandum suggested that the Garrison Commander prepare a plan of action to consolidate installation operational contingency plans that would incorporate Y2K issues. The Garrison Commander concurred with the assessment results and suggestions stated in the memorandum.

Memorandum Report No. AA 00-82, "Audit of Critical Weapon Systems - Year 2000; Assessment of the Paladin Self-Propelled Howitzer (M109A6) at the U.S. Army Tank-automotive and Armaments Command," November 29, 1999. The memorandum stated that command personnel had made significant progress toward ensuring Y2K compliance of the Paladin. Through the operational evaluation performed at the Army Communications-Electronics Command's Fire Support Software Engineering Center at Fort Sill, Oklahoma, command personnel had adequately certified and documented Y2K compliance for the Paladin. The memorandum did not contain any suggestions. Command personnel agreed with the conclusion stated in the memorandum.

Memorandum Report No. AA 00-75, "Audit of Automated Information Systems - Year 2000; Assessment of the Army Authorization Document System at the U.S. Army Force Management Support Agency," November 24, 1999. The memorandum stated that command personnel certified the Army Authorization Document System as Y2K compliant. In addition, command personnel exceeded their November 15, 1999 full implementation milestone as reported to the Army. Full fielding for this mission-critical system was completed on November 1, 1999. Command personnel agreed with the results stated in the memorandum. There were no suggestions made and there were no outstanding issues.

Memorandum Report No. AA 00-74, "Audit of Automated Information Systems - Year 2000; Assessment of the Unit Level Logistic System-Aviation at the Program Executive Officer for Standard Army Management Information Systems," November 17, 1999. The memorandum stated that personnel had certified the Unit Level Logistic System-Aviation as Y2K compliant and had met the November 15, 1999, full implementation milestone reported to the Army. However, during the review, the Army Audit Agency identified some issue and risk areas that hindered responsible personnel from efficiently and effectively tracking the full implementation status for the Unit Level Logistic System-Aviation.

The memorandum suggested that the Director, Information Systems, Command, Control, Communications and Computers, establish reporting policies and procedures directed towards central sites for the implementation of software change packages. Specifically, the Director, Information Systems, Command, Control, Communication and Computers, should require central cites to report to the Project Manager the following elements by December 17, 1999:

- acknowledge receipt of change packages,
- functional or technical problems (operational capability), and
- completion of full implementation.

Personnel waived the outbrief regarding the results and conclusion.

Memorandum Report No. AA 00-73, "Audit of Automated Information Systems - Year 2000; Assessment of the Distributive Training Technology Project at the National Guard Bureau Program Executive Office for Information Systems," November 18, 1999. The memorandum stated that personnel provided reasonable assurance supporting Y2K compliance for the Distributive Training Technology Project. No suggestions were made and there were no outstanding issues.

Memorandum Report No. AA 00-59, "Audit of Automated Information Systems - Year 2000; Assessment of the Range and Training Land Program-Automated System," November 8, 1999. The memorandum stated that personnel provided reasonable assurance supporting Y2K compliance for the Range and Training Land Program-Automated System. However, the certification checklist was not reviewed and approved at the appropriate levels.

The memorandum suggested that the Commander, U.S. Army Corps of Engineers, have the Range and Training Land Program-Automated System Y2K Certification Checklist reviewed and approved at the appropriate levels.

The Corporate Information Center and Corps personnel concurred with the results and suggestion identified and stated that personnel initiated actions to correct and address the suggestion in the memorandum.

Memorandum Report No. AA 00-54, "Audit of Automated Information Systems - Year 2000; Assessment of Selected Mission Critical Systems at the National Guard Bureau Program Executive Office for Information Systems," November 29, 1999. The memorandum report stated that the Army Audit Agency concluded that the Project Management Office had addressed the issue and risk areas identified during its initial assessment, and provided reasonable assurance supporting Y2K compliance for the Reserve Component Automation System and the Retirement Points Accounting Management System. The memorandum report also stated that Project Management Personnel adequately certified Y2K compliance for the Retirement Points Accounting Management System and provided assurance it would meet or exceed the December 15, 1999, full implementation milestone reported to the Department of the Army. Program Executive Office personnel concurred with the results and conclusions stated in the report.

Memorandum Report No. AA 00-46, "Audit of Year 2000 Facility Infrastructure (Non-Information Technology); Assessment of the U.S. Army Training and Doctrine Command," November 10, 1999. The memorandum stated that command and installation personnel were engaged in managing Y2K facility infrastructure issues to ensure continuity of operations for mission-essential functions at installations. Specifically, command personnel exercised due diligence in centrally managing the command's Y2K oversight program for installation infrastructure continuity of operations. Also, installation personnel had provided assurance that they were addressing continuity of operations for facility infrastructure Y2K risks.

The Deputy Chief of Staff for Base Operations Support, the Deputy Chief of Staff for Information Management, and the Office of Internal Review and Audit Compliance agreed with the results of the report.

Memorandum Report No. AA 00-26, "Audit of Automated Information Systems - Year 2000; Assessment of Selected Mission Critical Systems at the U.S. Army Simulation, Training and Instrumentation Command," October 22, 1999. The memorandum stated that personnel provided reasonable assurance supporting Y2K compliance for the Corps Battle Simulation, Close Combat Tactical Trainer, Joint Readiness Training Center-Instrumentation System, National Training Center-Instrumentation System, and the Combat Maneuver Training Center-Instrumentation System.

The memorandum suggested that the Commander, Simulation, Training & Instrumentation Command (US Army), follow-up with support contractors to determine the status of the 45 contractors who did not respond to the survey about Y2K compliance, who the six support contractors were that initially reported noncompliant and their present status, and how the current status of the six support contractors would affect the Simulation, Training & Instrumentation Command (US Army) mission. The Army Audit Agency outbriefed command personnel on October 22, 1999.

Memorandum Report No. AA00-22, "Audit of Automated Information Systems - Year 2000; Assessment of Selected Army Air Traffic Control Mission Critical Systems," October 15, 1999. The memorandum stated that responsible command personnel took the necessary corrective actions to address earlier reported suggested actions, and provided reasonable assurance supporting Y2K compliance for the Radar Surveillance Central and Tactical Terminal

Control System. The issues corrected included preparation of contingency plans, correct assessments and reporting of mission-critical systems, and proper oversight for Non-Army managed Y2K mission-critical systems. No management comments were required.

Memorandum Report No. AA00-13, "Audit of Mission Critical Weapon Systems - Year 2000; Assessment of the Mobile Subscriber Equipment at the Office of the Program Executive Officer for Command, Control and Communications Systems," October 15, 1999. The memorandum stated that responsible personnel provided reasonable assurance supporting Y2K compliance for the Mobile Subscriber Equipment - Force Entry Switch, Node Center Switch, Large Extension Node, and the Small Extension Node. Six issue and risk areas concerning risk management, database accuracy, and contingency plans were identified during the audit. Responsible command personnel took action to resolve all issues and mitigate all risk areas.

Memorandum Report No. AA00-12, "Audit of Mission Critical Weapon Systems - Year 2000; Assessment of Selected Mission Critical Systems at the U.S. Army Criminal Investigation Command," October 15, 1999. The memorandum stated that the Electronic Imaging system, Automated Criminal Investigative Reporting System, Integrated Information Operating Strategy-Human Resources system and the Automated System Crime Records Center were considered Y2K compliant. The responsible personnel provided reasonable assurance supporting Y2K compliance for the four systems. However, there were two risk areas that required suggestions.

The memorandum suggested that the Commander, U.S. Army Criminal Investigation Division Command:

- update the Electronic Imaging system Contingency plans to incorporate the trigger date of October 7, 1999 for implementation of new contractor for drafting source codes, and

- obtain test results from Fort Lee (Government/Service provider) to support reported test results.

The U.S. Army Criminal Investigation Division Command concurred with the suggestions and stated that corrective actions had been completed.

Memorandum Report No. AA00-5, "Audit of Automated Information Systems - Year 2000; Assessment of the Resource Information System, Engineer, Reserve System at the Office of the Chief, Army Reserve," October 15, 1999. The memorandum stated that the Office of the Chief, Army Reserve, had certified and supported Y2K compliance for the Resource Information Systems, Engineer, Reserve System. The Army Audit Agency identified one risk area concerning upgrade delays resulting from delays in subordinate systems. Command personnel were able to mitigate the risk area; therefore, no command comments were required.

Memorandum Report No. AA99-428, "Audit of Mission Critical Weapon Systems - Year 2000; Assessment of Tactical Radio Communications Systems at the Office of Program Executive Officer, Command, Control and Communications Systems," September 20, 1999. The memorandum stated personnel from the Program Executive Office exercised due diligence and provided reasonable assurance supporting Y2K compliance of the Enhanced Position Location Reporting System and the Single Channel Ground and Airborne Radio System. Two risk areas identified during the audit involved updating the Y2K database and Y2K Certification Checklists to include present status and proper approval signatures. The project management office and the Army took corrective actions to eliminate the issues; therefore, no command comments were required.

Memorandum Report AA99-427, "Audit of Mission Critical Weapon Systems - Year 2000; Assessment of the Improved Guardrail V System at the U.S. Army Communications-Electronics Command," September 20, 1999. The memorandum stated that command personnel exercised due diligence and provided reasonable assurance supporting Y2K compliance for the Improved Guardrail V. Two risk areas required management attention: the current status of the Improved Guardrail V system in the Army Y2K Database and the completion of the Y2K Certification Checklist. Command personnel took appropriate action to resolve both issues; therefore, no command comments were required.

Memorandum Report No. AA99-423, "Audit of Automated Information Systems - Year 2000; Assessment of Selected Mission Critical Systems at the U.S. Army Reserve Personnel Command," September 22, 1999. The memorandum stated that command personnel adequately certified and supported Y2K compliance of the Reserve Database Maintenance System, Mobilization Personnel Processing System, and Automated Orders and Resource System. Four issue and risk areas were identified during the audit. The Army Audit Agency identified four risk areas dealing with interface testing and interface agreements. Command personnel corrected three of the risk areas and the remaining risk area was mitigated by DFAS. No comments were required of U.S. Army Reserve Personnel Command.

Memorandum Report No. AA99-422, Audit of Mission Critical Weapons Systems - Year 2000; Assessment of the Forward Area Air Defense Command and Control System at the Office of the Program Executive Officer for Command, Control and Communications Systems," September 20, 1999. The memorandum stated that the personnel from the Program Executive Office exercised due diligence and provided reasonable assurances supporting Y2K compliance for the Forward Area Air Defense Command and Control System. The Army Audit Agency identified four risk areas; interface testing, reporting issues, documentation of workarounds, and documentation of contracts. Project Management Personnel took action to resolve the four risk areas; therefore, no command comments were required.

Memorandum Report No. AA99-421. "Audit of Mission Critical Weapon Systems - Year 2000; Assessment of Mobile Subscriber Equipment at the U.S. Army Communications Electronics Command," September 20, 1999. The memorandum stated that command personnel have provided reasonable assurance supporting Y2K compliance for the Mobile Subscriber Equipment Network Planning Terminal and the Mobile Subscriber Equipment System

Control Center. Six issue and risk areas were identified in the report. Four risk areas including contingency plans, properly assessed software, risk management plans, and certification checklists were corrected during the audit. Two issues required suggestions.

The memorandum suggested that the Commander, U.S. Army Communications-Electronics Command review and approve the Y2K Certification Checklists for the AN/UYK-100 and the AN/TYQ-46 and obtain test plans, procedures and results from the contractor performing the Y2K compliance test on the Mobile Subscriber Equipment-Network Planning Terminal. Command personnel concurred with the suggestions and stated actions had been taken in response to the recommendations.

Naval Audit Service

Memorandum: "Review of Year 2000 Processing Problem in the Department of the Navy," Naval Space Command (NAVSPACECOM), November 22, 1999. The memorandum stated that the Naval Audit Service considered NAVSPACECOM's mission-critical systems to be complete. NAVSPACECOM reported the Shore Infrastructure Systems, Devices, and Infrastructure for all components in its claimancy to the Chief of Naval Operations. The Shore Infrastructure Systems, Devices, and Infrastructure for all sites were complete, except for the Intrusion Detection System. As a result, the Naval Audit Service considered the NAVSPACECOM Shore Infrastructure Systems, Devices, and Infrastructure to be in the implementation phase.

The Naval Audit Service recommended that NAVSPACECOM provide the status of the two incomplete components of the NAVSPACECOM Mission Processing Systems, which were the Configuration Management Tool and the Intrusion Detection System, to the Naval Audit Service by November 30, 1999 via the Department of the Navy Chief Information Officer and the Office of the Chef of Naval Operations Y2K office.

Memorandum: "Assessment of Department of the Navy's Success in Identifying and Mitigating Risks and Threats to the Navy's Continuity of Operations Relating to Year 2000," Naval Sea Systems Command (NAVSEA) - November 22, 1999. The memorandum stated that the Naval Audit Service considered the four NAVSEA systems that would not undergo additional operational evaluation to be complete. The four systems are the Technical Support System, the Integrated Survivability Management System, the Automated Explosive Ordnance Disposal Publication System, and the Ship Configuration and Logistics Support System. However, NAVSEA needed to improve the contingency plans for the Automated Explosive Ordnance Disposal Publication System and the Ship Configuration and Logistics Support System.

The Naval Audit Service recommended that NAVSEA rewrite the contingency plans for the two systems to include specific procedures to follow in the event of a Y2K problem to ensure continuing operation. The Naval Audit Service also recommended that NAVSEA provide an updated status report to the Naval Audit Service via the Department of the Navy Chief Information Officer and the Office of the Chief of Naval Operations Y2K Office by November 30, 1999.

Memorandum: "Review of the Processing Problem in the Department of the Navy," Naval Air System Command (NAVAIR), September 29, 1999. The memorandum stated that the Naval Audit Service considered the NAVAIR mission-support and mission-critical late systems, with the exception of five systems, to be in the implementation phase. The Naval Audit Service also considered NAVAIR Shore Infrastructure Systems, Devices, and Infrastructure to be in the completed phase.

In addition, the Naval Audit Service considered ten mission-critical and eight mission support systems in the implementation phase because of ship nonavailability. Most of these systems were scheduled for completion by December 31, 1999. However, the Naval Audit service suggested that because of time constraints more emphasis needed to be placed on deployed ships, aircraft, and shore locations.

Specific recommendations for NAVAIR were:

- complete all system installations by December 31, 1999;
- write, modify, revise, and test contingency plans including specific procedures to follow in the case of Y2K difficulties;
- rewrite and test the Tactical Automated Mission Planning System contingency plan to address stand-alone operation;
- certify that the current version of the Workload Planning System and the Common Workload Planning System is considered Y2K compliant;
- develop and test contingency plans for the Stars Download System in accordance with the Department of the Navy Chief Information Officer Y2K Action Plan; and
- contact users to get mail-out software installed.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Naval Computer and Telecommunications Command (NCTC) – September 21, 1999. The memorandum stated that the Naval Audit Service considered NCTC to be in the completed phase for their mission-critical systems and the implementation phase for its mission-support systems with the exception of one mission-critical system in the implementation phase and one mission-support system in the renovation phase. All systems were scheduled to be completed by December 31, 1999. Also, NCTC reported the Shore Infrastructure Systems, Devices, and Infrastructure for all sites as complete.

The Naval Audit Service recommended that NCTC:

- evaluate the status of the Inter-American Naval Telecommunications Network mission-support system and determine if November 10, 1999, was a reasonable completion date;
- request the NCTC immediate Superior in Command to provide accelerated assistance to the Inter-American Naval

Telecommunications Network Inter-American Naval Telecommunications Network system because of potential international ramifications to the Navy;

- accelerate the renovation of Inter-American Naval Telecommunications Network and request the Chief of Naval Operations provide additional resources to ensure that the Inter-American Naval Telecommunications Network system would be complete by December 31, 1999; and

- provide the results of the negotiation with the Office of the Chief of Naval Operations Y2K Office over the level of certification for the various telephone switches to the Naval Audit Service.

Memorandum: "Review of Year 2000 (Y2K) Processing in the Department of the Navy," Naval Sea Systems Command's (NAVSEA) Program Executive Office Team for Submarine (TEAM SUB) - September 2, 1999. The memorandum stated that the Naval Audit Service considered NAVSEA TEAM SUB to be in the completed phase for their mission-critical and mission support systems. TEAM SUB systems were complete with the exception of the three in the implementation phase because of ship non-availability. The Combat Control System, AN/WLR-8A High-Probability of Intercept Receiver, and Research and Development Sub Instrumentation Systems were scheduled to be completed by September 30, 1999. Also, TEAM SUB reported Shore Infrastructure Systems, Devices, and Infrastructure to be in the implementation phase.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Space and Naval Warfare Systems Command - September 2, 1999. The memorandum stated that the Naval Audit Service considered the Space and Naval Warfare Systems Command (SPAWAR) to be in the implementation phase for mission-critical and mission-support systems and Shore Infrastructure Systems, Devices, and infrastructure. SPAWAR had not met the Department of Defense and Department of the Navy's Y2K target completion dates for its mission-critical and mission-support systems and their Shore Infrastructure Systems, Devices, and infrastructure. SPAWAR was closely managing late systems and should have all systems completed by December 31, 1999.

The Naval Audit Service recommended that SPAWAR:

- report the status of the Cornet Black Analog Switch, STQ Family Switches, VME Integrated Communication system, and the Element Management system to the Naval Audit Service beginning September 30, 1999, and every month thereafter;

- continue tracking progress and coordinating implementation availability for the systems not yet completed;

- report the results of the Continuity of Operations Plan test to the Department of the Navy Chief Information Officer;

- increase efforts to complete the Commanders Tactical Terminal Hybrid 3 Channel system and report status monthly to the Naval Audit Service; and

- report monthly status of Facilities and Infrastructure to the Naval Audit Service via Office of the Chief of Naval Operations Y2K office and Department of the Navy Chief Information Officer offices beginning September 30, 1999.

Appendix B. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
  Principal Deputy Under Secretary for Acquisition, Technology, and Logistics
  Deputy Under Secretary of Defense (Environmental Security)
  Deputy Under Secretary of Defense (Industrial Affairs and Installations)
  Deputy Under Secretary of Defense (Logistics)
  Director, Defense Procurement
  Director, Defense Research and Engineering
  Director, Defense Logistics Studies Information Exchange
  Director, Strategic and Tactical Systems
  Director, Test Systems Engineering and Evaluation
  Assistant to the Secretary of Defense (Nuclear, Chemical, and Biological Defense Programs)
Under Secretary of Defense for Policy
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
  Director, Program Analysis and Evaluation
Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Assistant Secretary of Defense (Command, Control, Communications, Intelligence, Surveillance, Reconnaissance, and Space Systems)
  Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief Information Officer Policy and Implementation)
    Principal Director for Year 2000
Assistant Secretary of Defense (Health Affairs)
Assistant Secretary of Defense (Legislative Affairs)
Assistant Secretary of Defense (Public Affairs)
Director, Operational Test and Evaluation

Joint Staff

Director, Joint Staff

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Chief Information Officer, Department of the Army
Inspector General, Department of the Army
Auditor General, Department of the Army

Department of the Navy

Chief Information Officer, Department of the Navy
Naval Inspector General
Auditor General, Department of the Navy
Inspector General, Marine Corps

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Chief Information Officer, Department of the Air Force
Inspector General, Department of the Air Force
Auditor General, Department of the Air Force

Unified Commands

Commander in Chief, U.S. European Command
Commander in Chief, U.S. Pacific Command
Commander in Chief, U.S. Atlantic Command
Commander in Chief, U.S. Southern Command
Commander in Chief, U.S. Central Command
Commander in Chief, U.S. Space Command
Commander in Chief, U.S. Special Operations Command
Commander in Chief, U.S. Transportation Command
Commander in Chief, U.S. Strategic Command

Other Defense Organizations

Director, Ballistic Missile Defense Organization
  Chief Information Officer, Ballistic Missile Defense Organization
Director, Defense Advanced Research Projects Agency
  Chief Information Officer, Defense Advanced Research Projects Agency
Director, Defense Commissary Agency
  Chief Information Officer, Defense Commissary Agency
Director, Defense Contract Audit Agency
  Chief Information Officer, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
  Chief Information Officer, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
  Chief Information Officer, Defense Information Systems Agency
  Inspector General, Defense Information Systems Agency
  United Kingdom Liaison Officer, Defense Information Systems Agency
Director, Defense Legal Services Agency
  Chief Information Officer, Defense Legal Services Agency

Other Defense Organizations (cont'd)

Director, Defense Logistics Agency
  Chief Information Officer, Defense Logistics Agency
Director, Defense Security Assistance Agency
  Chief Information Officer, Defense Security Assistance Agency
Director, Defense Security Service
  Chief Information Officer, Defense Security Service
Director, Defense Threat Reduction Agency
  Chief Information Officer, Defense Threat Reduction Agency
Director, National Security Agency
  Inspector General, National Security Agency
Director, Washington Headquarters Services
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency
Inspector General, National Reconnaissance Office

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
  Office of Information and Regulatory Affairs
Technical Information Center, National Security and International Affairs Division, General Accounting Office
Director, Defense Information and Financial Management Systems, Accounting and Information Management Division, General Accounting Office

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Special Committee on the Year 2000 Technology Problem
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, International Relations, Committee on Government Reform
House Subcommittee on Technology, Committee on Science

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report.

Thomas F. Gimble
Mary L. Ugone
James W. Hutchinson
Amy L. Schultz
Mark J. Thomas
Paul D. Johnston

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Summary of DOD Year 2000 Issues IV

B. DATE Report Downloaded From the Internet: 02/07/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 02/07/99**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.